為SEG配置按策略掃描的威脅掃描程式

目錄

簡介

必要條件

- 採用元件

概觀

設定

- Web介面設定
- 命令列介面設定

驗證

相關資訊

簡介

本文檔介紹思科安全郵件網關(SEG)的每個策略整合的威脅掃描器(TS)的服務和配置。

必要條件

需要瞭解SEG一般設定和配置。

採用元件

本檔案中的資訊是根據以下軟體版本：

- Cisco Secure Email Gateway (SEG) AsyncOS 15.5.1及更高版本。
- 灰色郵件服務。
- 反垃圾郵件服務。
- 傳入郵件策略。

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

概觀

威脅掃描(TS)是Graymail服務新啟用的子元件，已與Antispam CASE整合，可提供更有效的反垃圾郵件檢測。

啟用灰色郵件服務後，每個傳入郵件策略AntiSpam設定中啟用威脅掃描器的選項均會變為活動狀態。啟用TS後，TS將加強整體反垃圾郵件檢測，重點是HTML走私檢測：

- HTML解析和惡意指令碼檢測
- URL解析和重定向檢測

Antispam CASE引擎管理這兩種服務，管理更新和垃圾郵件定罪。

TS在每個傳入郵件策略反垃圾郵件設定中都顯示啟用/停用設定。

TS影響判決，增加了最終反垃圾郵件案例判決的權重。

設定

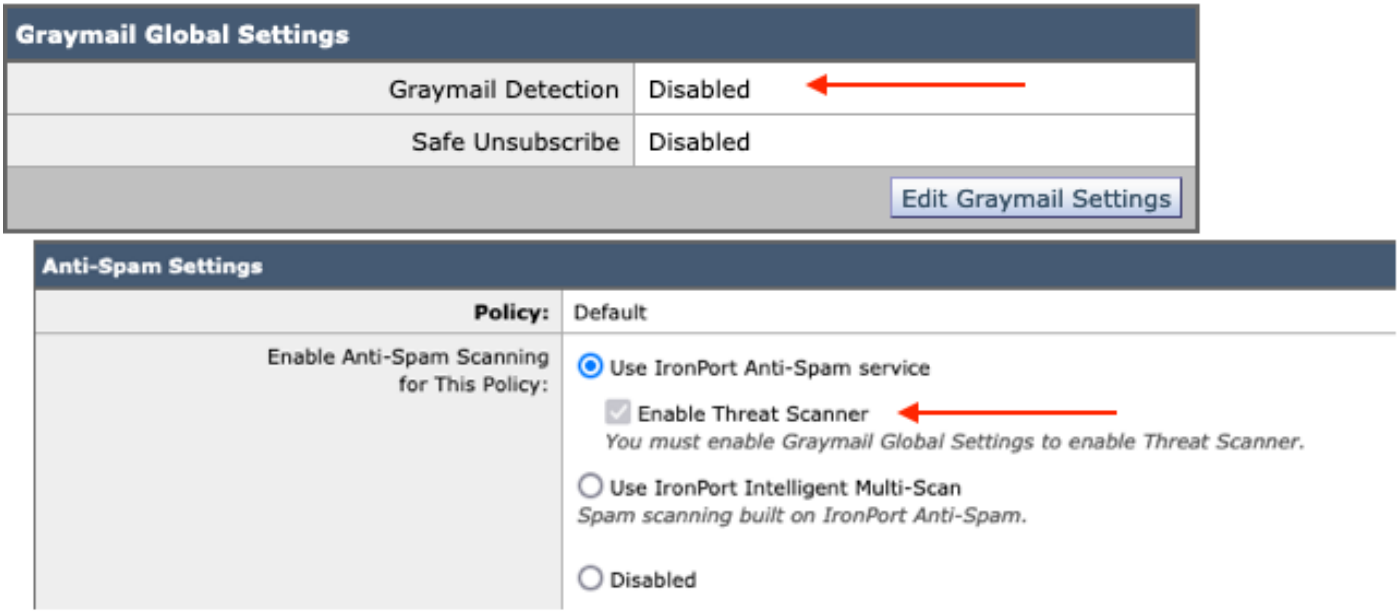
配置包含兩個操作：「啟用灰色郵件檢測」和「啟用傳入郵件策略中的TS」。

- 必須啟用Graymail全局服務才能啟用TS。
- 全局啟用灰色郵件後，入站郵件策略「反垃圾郵件」選項「啟用威脅掃描程式」將變為可用。

Web介面設定

若要在WebUII中啟用灰色郵件：

- 導航到安全服務
  - IMS和灰色郵件
    - 灰色郵件全局設定
      - 編輯灰色郵件設定。
        - 選擇啟用灰色郵件檢測的選項。
- 提交並提交更改以最終完成操作。



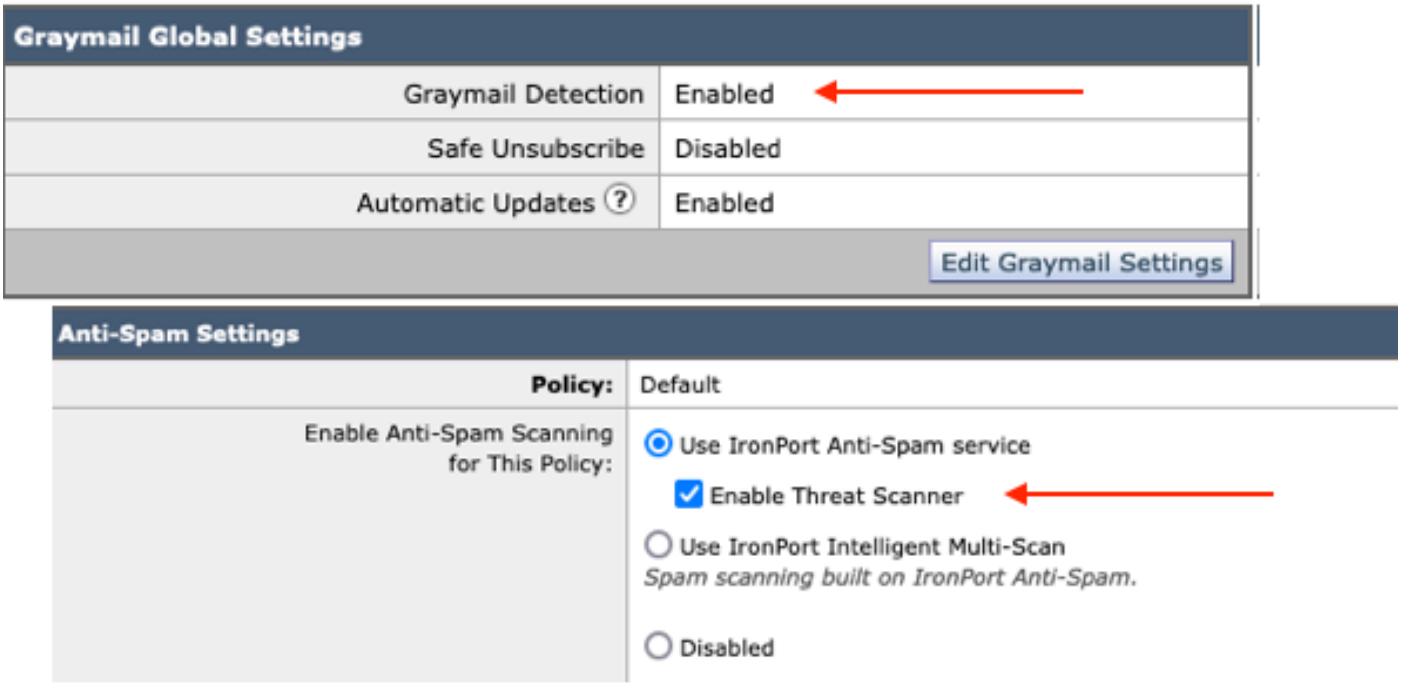
設定前的檢視

啟用Graymail後，威脅掃描程式選擇框將可用於每個傳入郵件策略。

要在WebUI中啟用威脅掃描程式，請執行以下操作：

- 導航到郵件策略
  - 傳入郵件策略
    - 選擇所需的郵件策略

        - 選擇Anti-Spam。
            - 配置頁面頂部顯示了用於啟用威脅掃描器的覈取方塊選項。
- 提交並提交更改以最終完成配置



Antispam中的威脅掃描程式選項

命令列介面設定

使用CLI命令啟用灰色郵件服務。

- imsandgraymailconfig
    - 灰色郵件
        - 設定
            - 是否要使用灰色郵件檢測？[Y] >
                - 是否要啟用灰色郵件引擎的自動更新？[Y]>
    - 完成其餘的提示以返回主機提示符。

- 提交+增加所需註釋>按「Return」鍵完成操作。

在CLI的策略中啟用或停用威脅掃描程式。

- CLI> policyconfig

是否要配置傳入郵件策略、傳出郵件策略或匹配郵件頭優先順序？

1. 傳入郵件策略
2. 外發郵件策略
3. 匹配報頭優先順序

[1]> 1

傳入郵件策略配置

1. 北部1
2. 阻止清單
3. ALLOWED_LIST
4. 允許_欺騙
5. 預設值

輸入您要編輯的專案的名稱或編號：
[]> 1

選擇要執行的作業：
- NAME -更改策略名稱
- NEW -增加新策略成員行
- DELETE -刪除策略成員行
- PRINT -列印策略成員行
- 反垃圾郵件-修改反垃圾郵件策略
- 防病毒-修改防病毒策略
- 爆發-修改爆發過濾器策略
- 高級惡意軟體-修改高級惡意軟體防護策略
- 灰色郵件-修改灰色郵件策略
- THREATDEFENSECONNECTOR -修改威脅防禦聯結器
- 過濾器-修改過濾器
[]>反垃圾郵件

選擇要執行的作業：
- DISABLE -停用反垃圾郵件策略（停用所有策略相關操作）
- ENABLE -啟用反垃圾郵件策略
[]>啟用

開始反垃圾郵件配置

是否要在此策略上使用智慧多掃描？[N]>

是否要在此策略上使用IronPort反垃圾郵件？[Y]>

某些郵件被明確標識為垃圾郵件。部分訊息為
辨識為可疑垃圾郵件。您可以設定IronPort反垃圾郵件疑似垃圾郵件
低於閾值。
配置選項適用於標識為
垃圾郵件：
是否要為威脅掃描程式判定啟用特殊處理？[N]> y

繼續選擇選單以完成郵件策略選擇，然後按「return鍵」接受每個選擇的預設操作。

使用指令完成儲存。

- 提交+增加所需註釋>按「Return」鍵完成操作。

驗證

如何閱讀和解釋日誌。

威脅掃描程式郵件記錄僅提供臨時裁決，而CASE提供最終裁決。

郵件日誌顯示了兩種不同的乾淨與已定罪威脅掃描程式裁決版本

- 如果威脅掃描程式臨時判定無誤，則日誌的顯示方式與這些示例類似。
  - 資訊：臨時灰色郵件裁決- LEGIT (0) <正常郵件>
  - 資訊：臨時灰色郵件裁決- MCE (11) <其他電子郵件活動>
- 如果威脅掃描程式臨時判定有罪，則日誌的顯示方式與這些示例類似。
  - 資訊：臨時ThreatScanner裁決-網路釣魚(101)
  - 資訊：臨時ThreatScanner裁決-病毒(2)

郵件日誌示例：威脅掃描程式Clean裁決使用不同的措辭：灰色郵件裁決。

<#root>

```
Wed Jan 31 08:19:32 2024 Info: MID 3189755
```

interim graymail verdict - LEGIT (0) <Clean message>

```
Wed Jan 31 08:19:33 2024 Info: MID 3189755 interim verdict using engine: CASE negative
Wed Jan 31 08:19:33 2024 Info: MID 3189755 using engine: CASE spam negative
```

郵件跟蹤不顯示威脅掃描程式日誌條目，僅顯示CASE： Final Verdict。

威脅掃描程式(TS)的這些示例展示了4種判定場景。

注意：「網路釣魚」和「病毒」的TS類別是唯一能夠增加案例判定分量的檢測

郵件日誌示例：存在網路釣魚TS定罪和AntiSpam定罪

<#root>

```
Thu Jan 25 09:05:23 2024 Info: MID 3057397
```

interim

ThreatScanner verdict - PHISHING (101)

```
 <Message detected as phishing either by heuristic analysis or by detecting the link as fraudulent>
Thu Jan 25 09:05:23 2024 Info: MID 3057397 interim verdict using engine: CASE spam positive
Thu Jan 25 09:05:23 2024 Info: MID 3057397
```

using engine: CASE spam positive

```
Thu Jan 25 09:05:23 2024 Info: Message aborted MID 3057397 Dropped by CASE
```

跟蹤示例：不存在網路釣魚TS定罪且存在CASE定罪。

25 Jan 2024 07:05:23 (GMT -08:00)	Message 3057397 matched per-recipient policy DEFAULT for inbound mail policies.
25 Jan 2024 07:05:23 (GMT -08:00)	Message 3057397 scanned by Anti-Spam engine: CASE. Interim verdict: Positive
25 Jan 2024 07:05:23 (GMT -08:00)	Message 3057397 scanned by Anti-Spam engine: CASE. Final verdict: Positive

網路釣魚TS定罪和AntiSpam定罪跟蹤

郵件日誌示例：網路釣魚TS定罪和AntiSpam Negative均存在。

<#root>

```
Thu Jan 25 09:05:47 2024 Info: MID 3057413
```

interim ThreatScanner verdict - PHISHING (101)

```
 <Message detected as phishing either by heuristic analysis or by detecting the link as fraudulent>
Thu Jan 25 09:05:47 2024 Info: MID 3057413 interim verdict using engine: CASE spam negative
Thu Jan 25 09:05:47 2024 Info: MID 3057413
```

using engine: CASE spam negative

跟蹤示例：存在網路釣魚TS已定罪和AntiSpam陰性。

25 Jan 2024 07:05:47 (GMT -08:00)	Message 3057413 matched per-recipient policy DEFAULT for inbound mail policies.
25 Jan 2024 07:05:47 (GMT -08:00)	Message 3057413 scanned by Anti-Spam engine: CASE. Interim verdict: Negative
25 Jan 2024 07:05:47 (GMT -08:00)	Message 3057413 scanned by Anti-Spam engine CASE. Interim verdict: definitely negative.
25 Jan 2024 07:05:47 (GMT -08:00)	Message 3057413 scanned by Anti-Spam engine: CASE. Final verdict: Negative

郵件日誌示例：郵件日誌的病毒TS定罪和AntiSpam定罪示例。

<#root>

```
Thu Jan 25 13:37:16 2024 Info: MID 3066060 interim
```

ThreatScanner verdict - VIRUS (2)

```
 <Virus detected by ThreatScanner engine>
Thu Jan 25 13:37:16 2024 Info: MID 3066060 interim verdict using engine: CASE spam positive
Thu Jan 25 13:37:16 2024 Info: MID 3066060
```

using engine: CASE spam positive

```
Thu Jan 25 13:37:16 2024 Info: Message aborted MID 3066060 Dropped by CASE
```

跟蹤示例：不存在病毒TS定罪且存在AntiSpam定罪。

25 Jan 2024 11:37:16 (GMT -08:00)	Message 3066060 matched per-recipient policy DEFAULT for inbound mail policies.
25 Jan 2024 11:37:16 (GMT -08:00)	Message 3066060 scanned by Anti-Spam engine: CASE. Interim verdict: Positive
25 Jan 2024 11:37:16 (GMT -08:00)	Message 3066060 scanned by Anti-Spam engine: CASE. Final verdict: Positive
25 Jan 2024 11:37:16 (GMT -08:00)	Message 3066060 aborted: Dropped by CASE

郵件日誌示例：病毒TS定罪和AntiSpam Negative均存在。

<#root>

```
Jan 23 21:38:57 2024 Info: MID 3013692
```

interim ThreatScanner verdict - VIRUS (2)

```
 <Virus detected by ThreatScanner engine>
Jan 23 21:38:58 2024 Info: MID 3013692 interim verdict using engine: CASE spam negative
Jan 23 21:38:58 2024 Info: MID 3013692
```

using engine: CASE spam negative

跟蹤示例：不存在病毒TS定罪，並且存在AntiSpam陰性。

23 Jan 2024 19:38:57 (GMT -08:00)	Message 3013692 matched per-recipient policy DEFAULT for inbound mail policies.
23 Jan 2024 19:38:58 (GMT -08:00)	Message 3013692 scanned by Anti-Spam engine: CASE. Interim verdict: Negative
23 Jan 2024 19:38:58 (GMT -08:00)	Message 3013692 scanned by Anti-Spam engine: CASE. Final verdict: Negative

灰色郵件日誌包含威脅掃描程式判定結果以及支援內容，用於進行誤報質詢時的TALOS分析。

威脅掃描程式原始結果的存在導致Graymail日誌記錄更快速地滾動。為了解決此行為，已對灰色郵件日誌進行了SEG修改。

- AsyncOS 15.5將Graymail日誌檔案的預設日誌訂閱設定為20，以增加日誌保留。
  - 如果在升級時設定高於20，則不會更改日誌檔案設定。
- 輸入灰色郵件暫時判定訊息會在資訊層級顯示完整掃描原始結果。
- 所有其他郵件的灰色郵件掃描結果均顯示在調試級別。

相關資訊

- 電子郵件安全設定指南
- 用於支援指南的思科安全郵件網關啟動頁面

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。